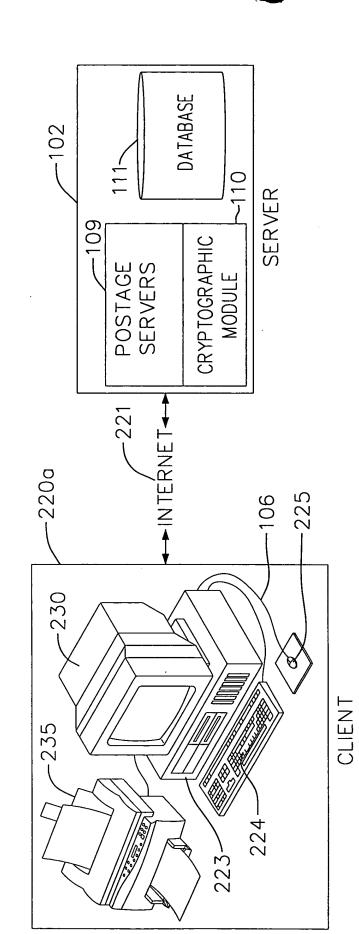
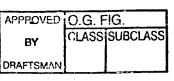
DOSCOPLE TOCHOL

FIG. 1

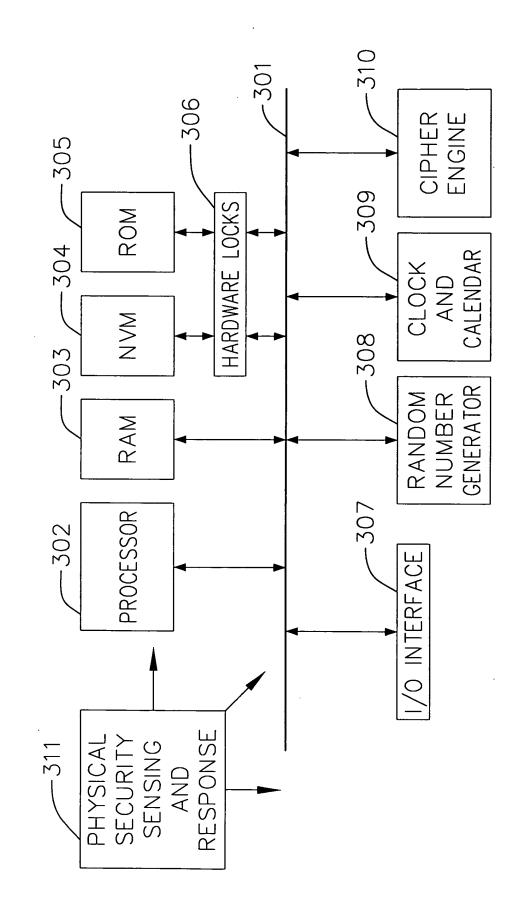




222a 222m SERVER • • • SERVER 234 221 -233n LOCAL NETWORK INTERNET -235 -233a -232n . 220n PRINTER COMM **NETWORK** LINK MONITOR 232a COMM FIG.2 ,231 230 227 MASS STORAGE MAIN MEMORY MONITOR VIDEO AMP 228 225 229 VIDEO MEMORY VIDEO AMP MOUSE 226 223 224 KEYBOARD CPU 

APPROVED O.G. FIG.		
BY	CLASS	SUBCLASS
DRAFTSMAN		

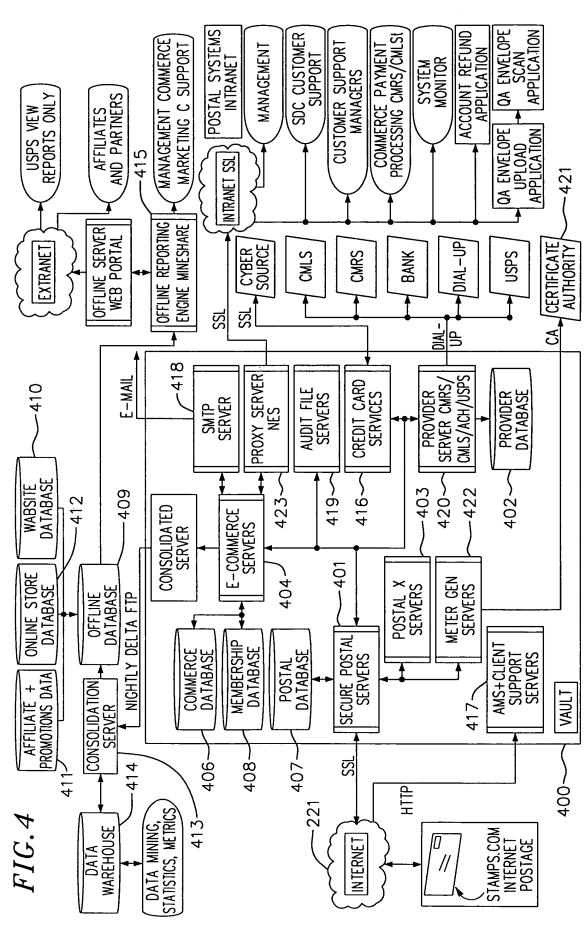
FIG.3



ĻŲ

iĒ

-4



APPROVED O.G. FIG CLASSISUBCLASS BY DRAFTSMAN

## FIG.5

GENERATES A RANDOM, 64-BIT CHALLENGE CLIENT SOFTWARE

THE CHALLENGE IT SENT WITH COMPARES THE HMAC OF THE HMAC IT RECEIVES CLIENT SOFTWARE FROM THE PSD.

CHALLENGE

SOFTWARE

CLIENT

RESPONSE

-503

-503

 HOST TRUSTS THE PSD FOR THIS TRANSACTION.

CHALLENGE TO AUTHENTICATE HOST RETAINS PSD'S ITSELF TO THE PSD

505-

CUSTOMER'S ASCENDING AND SIGNS CHALLENGE THAT THE PSD SENT, AND ALSO THE LOCAL RECORD OF THE DESCENDING REGISTERS. SENDS THIS TO PSD. CLIENT SOFTWARE

SENDS AN HMAC OF ALL OF SENDS CLEARTEXT OF THE RANSACTION MESSAGE. CHALLENGE AND THE

THE ABOVE, USING SHARED

 PSD RETURNS ABOVE, AS WELL
 AS ITS OWN 64-BIT CHALLENGE SHARED DURING REGISTRATION CHALLENGE, USING THE HMK • THE PSD SIGNS THE HOST'S ESTABLISHING TRUST BETWEEN HOST AND PSD FOR THE TRANSACTION 502 (CRYPTOGRAPHIC MODULE) PS

CHALLENGE

-501

SOFTWARE

CLIENT

CALCULATION OF THE SAME. WAS NOT TAMPERED WITH. THIS ENSURES MESSAGE RESPONSE WITH LOCAL COMPARES HASH OF PSD

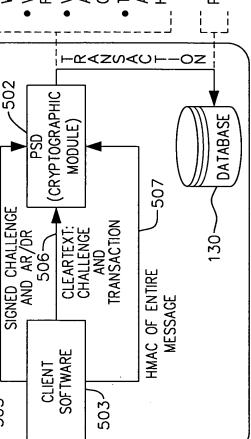
ESTABLISHING TRUST BETWEEN PSD AND HOST FOR THE TRANSACTION

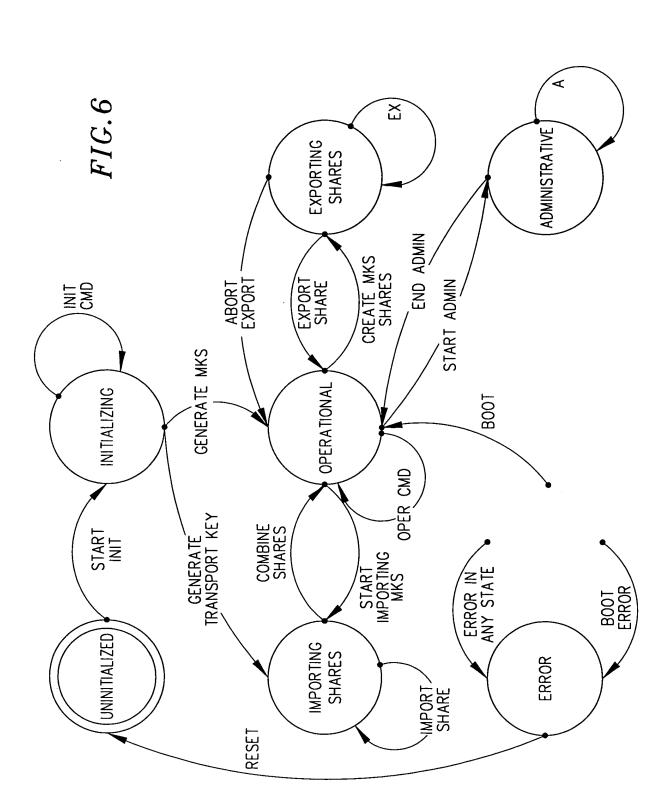
502

RECEIVED IS CHALLENGE SENT. VERIFIES HOST'S REGISTERS VERIFIES CHALLENGE

ARE SAME AS LOCAL DATA OF REGISTERS.

THIS ABOVE TWO STEPS AUTHENTICATE THE PSD PERFORMS TRANSACTION





H .= 

:5

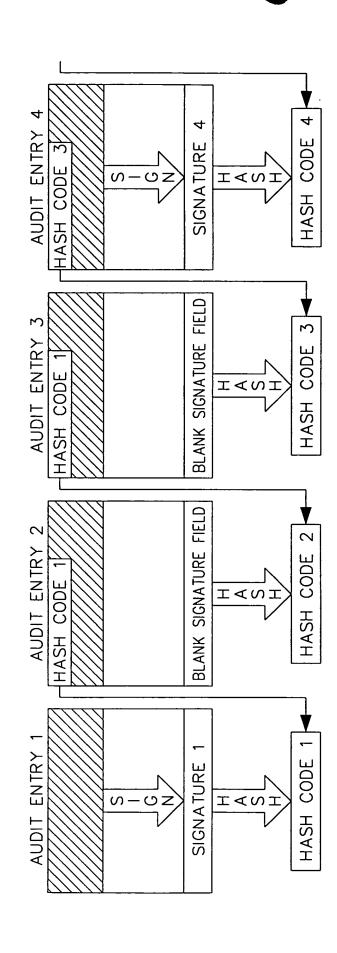
ļ.**d** 

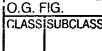
APPROVED O.G. FIG.

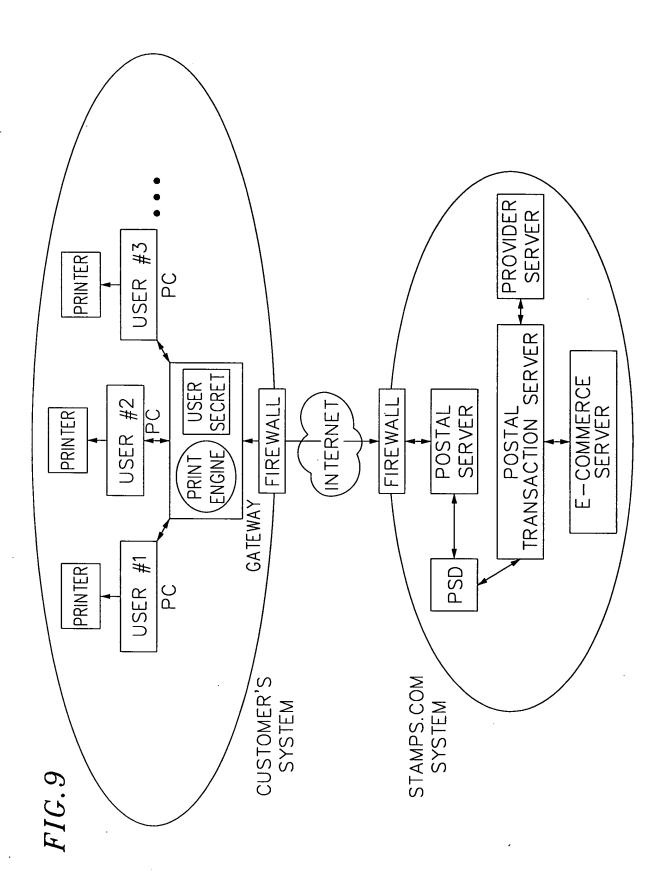
BY CLASS SUBCLASS

DRAFTSMAN

FIG 7







11 |-±

|-± ||T

FIG. 10

